



ROBIDUS



# Informatiebeveiliging en Privacy

[robidus.nl](https://www.robidus.nl)



# VOORWOORD

De wereld waarin we leven digitaliseert snel en de ontwikkelingen volgen elkaar in rap tempo op. Daardoor spelen informatiebeveiliging en privacybescherming een steeds belangrijkere rol in de samenleving.

Voor Robidus is dit niet anders. Ook wij werken steeds meer online en voor de uitvoering van onze dienstverlening verwerken we veel gevoelige informatie, waaronder persoonlijke gezondheidsgegevens. Dit zijn gegevens die we goed willen én moeten beschermen.

Wij nemen de bescherming van deze gegevens serieus en nemen passende technische en organisatorische maatregelen om misbruik, verlies, onbevoegde toegang, ongewenste openbaarmaking en ongeoorloofde wijziging tegen te gaan.

Hoe we dat doen? Dat leest u in dit document.



# INLEIDING

Robidus is een dienstverlener die werkgevers helpt bij het beperken van de risico's van verzuim en arbeidsongeschiktheid door optimale benutting van wettelijke regelingen en het sturen op inzetbaarheid. In het kader van de uitvoering van deze dienstverlening verwerken we persoonsgegevens. Hieronder vallen bijvoorbeeld NAW en contactgegevens, maar ook gegevens over de gezondheid van uw werknemers, zoals het re-integratiedossier van een zieke werknemer.

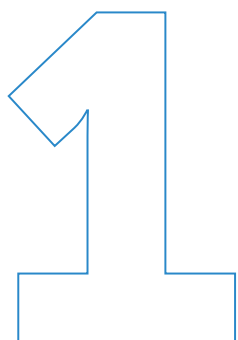
Bij de uitvoering van onze dienstverlening hebben we te maken met verschillende uitvoeringspartijen, zoals het UWV, de Belastingdienst, verzekeraars, re-integratiepartijen en bedrijfsartsen. Samen met deze partijen zorgen wij voor een praktische en efficiënte uitvoering van onze dienstverlening, binnen het kader van de geldende wet- en regelgeving op het gebied van sociale zekerheid.

In dit document benoemen we de maatregelen die we nemen om uw data te beschermen. Zowel qua beveiliging van onze systemen, maar ook in onze processen. Individuen zijn vaak de meest kwetsbare factor in het beveiligingsproces vandaar dat we ook uitgebreid toelichten welke interne maatregelen we treffen om de risico's op data-incidenten te minimaliseren. Of de uitvoering van onze aanpak juist is, laten we jaarlijks toetsen door externe specialisten.

Wij vertrouwen erop dat dit document voldoende inzicht biedt rondom onze beveiligingsmaatregelen. Heeft u toch nog vragen, dan kunt u ons bereiken via [compliance@robidus.nl](mailto:compliance@robidus.nl).

# INHOUDSOPGAVE

<b>1.</b>	<b>Onze 10 speerpunten</b>	<b>5</b>
<b>2.</b>	<b>Governance</b>	<b>7</b>
2.1	Assurance	7
2.2	Beleid	8
<b>3.</b>	<b>Informatiebeveiliging</b>	<b>9</b>
3.1	Toegangsbeveiliging	9
3.2	Personeel	10
3.3	Software ontwikkeling in eigen beheer	11
3.4	Testen	11
3.5	Databeheer en infrastructuur	13
3.6	Continuïteit	15
3.7	Issuemanagement	16
<b>4.</b>	<b>Privacy</b>	<b>17</b>
4.1	Verwerkingsverantwoordelijkheid	17
4.2	Grondslag	17
4.3	Doelbinding & noodzakelijkheid	17
4.4	Bewaartermijnen	18
4.5	Subverwerkers	19
4.6	Rechten van betrokkenen	19



# ONZE 10 SPEERPUNTEN

## 1. ISO CERTIFICERINGEN

Robidus is ISO 27001 en NEN 7510 gecertificeerd. Dit geeft u het vertrouwen dat beschikbaarheid, integriteit en vertrouwelijkheid van uw data geborgd zijn.

## 2. CYBER SECURITY

Cyberweerbaarheid, informatiebeveiliging en compliance zijn de fundamenten van onze ICT-architectuur. Wij nemen technische maatregelen zoals een managed IP-VPN, firewalls, Intrusion Detection & Prevention (IDP). Jaarlijks laten we de effectiviteit hiervan toetsen door externe partijen.

## 3. CONTINUÏTEIT

De hosting van onze systemen en data is uitbesteed aan een gespecialiseerde cloud solutions provider met redundant uitgevoerde data centers. Aanvullend heeft Robidus een disaster recovery plan voor bedrijfskritische applicaties om de continuïteit te garanderen. Dit plan wordt jaarlijks getest.

## 4. FYSIEKE EN LOGISCHE TOEGANGSBEVEILIGING

Zowel voor de kantoren als systemen is toegang ingeregeld volgens de principes 'need to know' en 'need to use', zodat uw data altijd alleen toegankelijk is voor onze medewerkers die hier vanuit hun takenpakket toegang toe moeten hebben.

## 5. ISSUE- EN ACTIEMANAGEMENT

Met ons issuemanagementproces zorgen we dat we incidenten met uw data tijdig signaleren en de impact ervan beperkt blijft. Een oorzakanalyse en structurele verbetering zijn standaard onderdeel van ons issue- en actiemanagementproces.

## **6. PERSONEEL**

Menselijke handelingen zijn vaak de kwetsbare factor bij de beveiliging van data. Daarom stimuleert Robidus bewustzijn, opleiding en training ten aanzien van informatiebeveiliging.

## **7. DATAVERWERKING**

Om de privacy van uw werknemers optimaal te kunnen borgen, verwerkt Robidus data alleen in landen waar de Algemene Verordening Gegevensbescherming (AVG) van kracht is. Bovendien spreekt Robidus met al haar leveranciers af dat zij dit ook doen.

## **8. PRIVACY PRINCIPES**

Robidus ontwikkelt software in eigen beheer. Hierbij werken wij volgens de principes 'privacy by design' en 'privacy by default'. Daarmee zorgen we dat de vertrouwelijkheid van uw data zowel technisch als organisatorisch geborgd is.

## **9. AVG-BEGINSELEN GEBORGD**

Robidus verwerkt alleen die data, die noodzakelijk is voor de uitvoering van dedienstverlening die u bij ons afneemt. Daarbij zorgen wij ervoor dat wij uw data nooit langer bewaren dan nodig.

## **10. AFSPRAKEN OVER PRIVACY VASTGELEGD**

Wij borgen informatiebeveiliging en privacy door voorafgaand aan en tijdens de samenwerking met leveranciers beoordelingen uit te voeren en verwerkersovereenkomsten te sluiten.

# 2 GOVERNANCE

De kern van onze maatregelen om uw data te beschermen ligt besloten in internationale standaarden. De naleving van deze standaarden is verankerd in het Robidus DNA.

## 2.1 ASSURANCE

Robidus is er trots op dat wij beschikken over twee certificeringen en één assurancerapport waarmee wij aantonen te voldoen aan internationale kwaliteitsstandaarden op het gebied van informatiebeveiliging en procesbeheersing.

### ISO 27001

De ISO 27001 is een internationaal erkende norm op het gebied van informatiebeveiliging. Deze certificering geeft u de zekerheid dat voor uw gegevens de beschikbaarheid, vertrouwelijkheid en integriteit geborgd is.



### NEN 7510

Robidus verwerkt gevoelige gezondheidsinformatie. Met de NEN 7510-certificering tonen wij aan dat onze informatiebeveiliging voldoet aan de specifieke eisen voor persoonlijke gezondheidsinformatie, zodat vertrouwelijkheid, beschikbaarheid en integriteit van deze gegevens gewaarborgd zijn.



### ISAE 3000

De ISAE 3000 is een internationaal erkende standaard, waarmee we naar onze relaties kunnen aantonen dat wij onze dienstverleningsprocessen beheersen en onze beheersmaatregelen naar behoren uitvoeren.



Jaarlijks controleert een externe organisatie of wij blijvend voldoen aan de gestelde eisen.

## 2.2 BELEID

Onze diverse beleidsdocumenten en processen zijn gebaseerd op bovenstaande standaarden. We noemen twee belangrijke beleidsdocumenten:

- Ons Informatiebeveiligingsbeleid is gebaseerd op relevante wet- en regelgeving en de eisen van onze partners en klanten. Dit beleid is het uitgangspunt om gerichte maatregelen te treffen, waarmee informatiebeveiligingsrisico's tot een passend niveau gereduceerd worden. Het beleid is opgesteld op basis van de ISO 27001 standaard. Tevens zijn relevante beheersmaatregelen uit onze ISAE 3000 rapportage opgenomen in dit beleid.
- Aanvullend op het Informatiebeveiligingsbeleid heeft Robidus het Privacybeleid. Dit beleid omschrijft hoe Robidus omgaat met de verwerking van persoonsgegevens en geeft daarmee uitvoering aan privacywetgeving, waaronder de AVG.

Om er zeker van te zijn dat een passend beschermingsniveau voor alle typen informatie geborgd is, zijn het Informatiebeveiligingsbeleid en Privacybeleid volledig op elkaar afgestemd.

# 3

## INFORMATIE- BEVEILIGING

**Informatiebeveiliging is essentieel. Niet alleen om de wetgeving na te leven, maar ook omdat het u en Robidus verder helpt. Wanneer data, processen en systemen te vertrouwen zijn dan minimaliseert dat de risico's.**

**In dit hoofdstuk omschrijven we wat Robidus doet om zorgvuldig om te gaan met uw data.**

### 3.1 TOEGANGBEVEILIGING

#### Systemen

Het toegangsbeheer tot de Robidus systemen gaat uit van de principes 'need to know' en 'need to use'. Hierdoor krijgen onze medewerkers alleen toegang tot de gegevens die noodzakelijk zijn voor de uitvoering van hun functie. Accounts met hoge rechten zijn tot een minimum beperkt en worden alleen toegekend aan gebruikers die dit nodig hebben uit hoofde van hun functie.

Er zijn processen ingericht die borgen dat bij indiensttreding, uitdiensttreding en verandering van functie de rechten toegekend, gewijzigd en/of ingetrokken worden.



Alle gebruikersaccounts zijn uniek herleidbaar tot een individuele medewerker. De gebruikersaccounts zijn beveiligd met Multi Factor Authentication (MFA; maturity level 3). Vastgestelde wachtwoordvereisten, zoals lengte, gebruik cijfers/tekens en regelmatig updaten, worden systeemtechnisch afgedwongen.



Robidus medewerkers kunnen vanaf een andere locatie werken. Ook daarbij nemen we strenge maatregelen in acht. Zo is toegang tot het Robidus netwerk vanuit andere netwerken alleen mogelijk met een VPN-verbinding. Deze verbinding maakt gebruik van MFA.



#### Kantooromgeving

Medewerkers verkrijgen toegang tot onze kantoorlocaties in Zaandam en Breukelen met behulp van een persoonsgebonden dongel. Leveranciers en bezoekers worden vooraf aangemeld en worden altijd begeleid door een medewerker. De kantoren zijn voorzien van camerabeveiliging.

## 3.2 PERSONEEL

Onze medewerkers geven uitvoering aan onze dienstverlening. Van hen verlangen wij dat zij hun uiterste best doen om veilig om te gaan met de informatie waarover zij beschikken. De bewustwording is een continu aandachtsgebied binnen onze organisatie.

### **Pre- en inemploymentscreening**

Alle kandidaten voor een dienstverband bij Robidus worden gescreend. Daarbij wordt onder meer een Verklaring Omtrent Gedrag (VOG) opgevraagd en beoordeeld. Daarnaast kijken we naar de aanwezigheid en geldigheid van verplichte diploma's en worden een aantal functie-specifieke controles uitgevoerd. Tijdens het dienstverband worden deze controles periodiek herhaald.

### **Awareness/Kennis**

Nieuwe medewerkers starten met een intensief onboardingprogramma. Informatiebeveiliging en privacy maken daarvan een belangrijk deel uit. Zij krijgen een presentatie over deze onderwerpen en nemen deel aan een verplichte e-learning.

Daarnaast is er voor medewerkers een uitgebreid awareness programma, bestaande uit onder meer een jaarlijks verplichte e-learning, kennissessies, nieuwsberichten op intranet, phishing simulaties, etc.

### **Geheimhoudingsverklaring**

Alle medewerkers tekenen bij indiensttreding een geheimhoudingsverklaring. Bij uitdiensttreding wordt de medewerker erop gewezen dat deze geheimhouding blijft gelden na uitdiensttreding. De medewerker tekent ervoor dat hij/zij zich hieraan zal houden.

Voor ZZP'ers en freelancers gelden dezelfde vereisten.

### 3.3 SOFTWARE ONTWIKKELING IN EIGEN BEHEER

Robidus ontwikkelt in eigen beheer een suite van SAAS-applicaties. Al deze omgevingen beschikken over een Ontwikkeling, Test, Acceptatie en Productie-omgeving (OTAP-straat), waarvan de verschillende omgevingen logisch van elkaar gescheiden zijn. Systeembeveiliging wordt in iedere stap van het proces getest.

De door Robidus ontwikkelde software houdt alle wijzigingen bij in een 'forensisch' log. Dit bestaat uit 3 onderdelen: een mutatielog, request-log en applicationerror log.

### 3.4 TESTEN

Robidus beschikt over testbeleid voor zowel de in eigen beheer ontwikkelde software als voor de infrastructuur. Dat beleid omvat diverse testen, waaronder een penetratietesten die ten minste jaarlijks of bij grote wijzigingen wordt uitgevoerd.

Eventuele bevindingen uit deze test worden direct beoordeeld. Dit gebeurt aan de hand van een checklist waarbij de impact qua informatiebeveiliging in kaart wordt gebracht. Indien nodig worden verbeteringen doorgevoerd, waarna een nieuwe test volgt.



#### **Cloudhosting**

Robidus verwerkt klantdata in de cloud via een Azure Landing Zone. Het beheer van deze omgeving is uitbesteed aan Solvinity, een gespecialiseerde Cloud Service Provider. Alle data wordt uitsluitend verwerkt binnen de Europese Economische Ruimte (EER) en redundant opgeslagen. De datacenters zijn TIER 3-geclassificeerd, waardoor onderhoud en vervanging van apparatuur zonder verstoring kan plaatsvinden. Monitoring en beheer zijn geborgd via een SLA met 24/7 toezicht op alle systemen, zodat continuïteit, beschikbaarheid en veiligheid gegarandeerd zijn.

### **Cyber Security weerbaarheid**

- We werken voor de Robidus-applicaties met een gecertificeerde partner voor secure managed cloud services. Alle data is gehost in Azure waarbij gebruik wordt gemaakt van redundant storage.
- Een managed en redundant IP VPN WAN tussen de kantoorlocaties en Azure Landing Zone.
- Toegang voor remote werken met een clientside VPN-oplossing en authenticatiebeveiliging op basis van account + MFA.
- Toegangsbeperking tot door Robidus ontwikkelde applicaties op basis van Federated Authentication, IP allow-listing of MFA



### **Gegevensuitwisseling**

Om de persoonsgegevens veilig en efficiënt te kunnen uitwisselen tussen uw organisatie en Robidus, maken we gebruik van onze eigen ontwikkelde Robidus Databeheer applicatie in combinatie met het koppelplatform NewDays.

Uitwisseling van gegevens gebeurt bij voorkeur geautomatiseerd. Gegevensuitwisseling kan op die manier sneller en veiliger. Indien dit niet mogelijk is, worden gegevens uitgewisseld via e-mail. Als e-mailberichten vertrouwelijke gegevens, waaronder persoonsgegevens, bevatten, worden e-mailberichten altijd extra beveiligd door gebruik te maken van de veilig mailen-applicaties Zivver en Filecap.

## 3.5 DATABEHEER EN INFRASTRUCTUUR



### Encryptie

De data op onze infrastructuur is versleuteld. De encryptiemethode is conform de geldige industry best practices op het gebied van encryptie.

Ter bescherming van vertrouwelijke informatie worden alle Robidus werkstations beveiligd d.m.v. het versleutelen van de gegevensdragers met beleidsregels volgens geldige industry best practices op het gebied van encryptie zoals gepubliceerd door NIST.

- Het werkstation beschikt over (minimaal) een Trusted Platform Module 2.0 chip. De encryptie software die wordt gebruikt is Microsoft Bitlocker.

Communicatie over het internet van en naar door Robidus ontwikkelde software vindt versleuteld plaats middels Secure Socket Layer (SSL), waarbij gebruik wordt gemaakt van een certificaat. Aan dit certificaat stelt Robidus de volgende inhoudelijke eisen:

- Er wordt gebruikgemaakt van RSA-encryptie waarbij de grootte van de private key conform de geldende best practices is vastgesteld.
- Het certificaat is verstrekt door een algemeen geaccepteerde autoriteit

### Anti-virus en anti-malware

Robidus geeft uitvoering aan het anti-virus en anti-malwarebeleid, met de volgende uitgangspunten:

- Het is verboden om ongeautoriseerde software te installeren, dit is technisch afgedwongen;
- Op alle computersystemen is anti-virus en anti-malware software aanwezig en alle in- en uitgaande e-mail wordt gecontroleerd op virussen en malware. De software wordt automatisch voorzien van nieuwe updates.

### Data-classificatie

Robidus verwerkt verschillende typen informatie, welke op verschillende wijzen adequaat worden beschermd. Hiertoe wordt onderstaand classificatieschema aangehouden:

Classificatie	Type	Omvat
I	<b>Vertrouwelijk</b>	Betreft alle persoonsgegevens waar Robidus voor haar dienstverlening mee werkt. Dit zijn gegevens welke naar individuele natuurlijke personen zijn te herleiden
0-b	<b>Intern</b>	Informatie die alleen bestemd is voor intern gebruik
0-a	<b>Publiek</b>	Alle applicaties waarin klantgegevens staan, hebben minimaal de classificatie vertrouwelijk.

Binnen de hierboven uitgewerkte classificatie, gaan we uit van de volgende uitgangspunten:

- Alle documenten uit de documenthiërarchie hebben minimaal de classificatie **intern**
- Alle applicaties waarvoor een wachtwoord nodig is, hebben minimaal de classificatie **intern**
- Alle applicaties waarin klantdata staan, hebben minimaal de classificatie **vertrouwelijk**.

## 3.6 CONTINUÏTEIT



### **Back-ups**

Robidus hanteert een strikt back-upbeleid om in geval van calamiteiten altijd een back-up beschikbaar te hebben. Back-ups worden beveiligd in lijn met ons Informatiebeveiligingsbeleid, waaronder versleutelde opslag van de back-ups.



### **Patchmanagement**

Een patch is een installatiebestand dat een kwetsbaarheid of fout in een programma herstelt. Om de risico's als gevolg van benutting van technische kwetsbaarheden te beheersen heeft Robidus de volgende maatregelen genomen:

- Patches voor kwetsbaarheden waarvan de kans op en impact van misbruik hoog is, worden zo spoedig mogelijk, maar minimaal binnen één week, uitgevoerd. Minder kritische beveiligingsupdates worden ingepland bij de eerstvolgende, reguliere onderhoudsronde van het betreffende systeem.
- Voor kritische applicaties waarvan het beheer uitbesteed is, zijn met leveranciers afspraken gemaakt over het beheer van kwetsbaarheden en patching van (systeem)software. Deze afspraken zijn ten minste gelijk aan het geldende interne beleid ten aanzien van patchmanagement.
- Periodiek wordt gecontroleerd of de installatie van de laatste patches is doorgevoerd.



### **Bedrijfscontinuïteit**

Om bij calamiteiten zo snel mogelijk weer onze dienstverlening aan u te kunnen leveren en gevoelige informatie veilig te houden, is Business Continuity Management ingericht. Beleid en processen hieromtrent worden jaarlijks en bij grote wijzigingen herzien. Er zijn calamiteitenplannen om in geval van een calamiteit direct te kunnen handelen. Deze plannen worden minimaal eens per jaar getest.

### 3.7 ISSUEMANAGEMENT

Robidus beschikt over een issuemanagementproces. Alle incidenten worden in lijn met dit proces geregistreerd en afgehandeld. We maken hierbij onderscheid tussen:

- Operationele incidenten, waaronder beveiligingsincidenten.
- Klachten (zowel intern als extern).
- Data-incidenten: incidenten waarbij persoonsgegevens betrokken zijn. Ook incidenten waarbij (nog) geen sprake is van een datalek, worden geregistreerd en afgehandeld.
- ICT-incidenten: ICT-incidenten die (mogelijk) een bredere impact hebben en/of waarvoor een bredere oplossing vereist is, worden geregistreerd.

De afdeling Legal, Risk & Compliance behandelt alle binnenkomende incidenten en analyseert en rapporteert periodiek over de oorzaken van de incidenten. Hierbij wordt tevens ingegaan op de lering welke getrokken is uit de incidenten en welke vervolgacties zijn ingezet om herhaling te voorkomen.

Onderdeel van het issuemanagementproces is het binnen 24 uur na constatering melden van het incident bij u. Hierbij informeren wij u over hetgeen zich heeft voorgedaan, de maatregelen die wij getroffen hebben en de maatregelen die wij nog gaan treffen.

# 4 PRIVACY

Privacy gaat over het recht van alle burgers op de bescherming van hun persoonlijke levenssfeer. Voor het uitvoeren van onze dienstverlening is gegevensverzameling en -uitwisseling van groot belang. Het beschermen van persoonsgegevens en een rechtmatige gegevensverwerking is een essentieel onderdeel hiervan. Robidus heeft privacy hoog in het vaandel staan: wij verwerken persoonsgegevens op een rechtmatige, zorgvuldige en transparante manier, conform wet- en regelgeving.

## 4.1 VERWERKINGSVERANTWOORDELIJKHEID

In de AVG wordt uitgegaan van twee rollen als het gaat om de verwerking van persoonsgegevens, namelijk de verwerkingsverantwoordelijke en de verwerker. Robidus is verwerker en voert haar dienstverlening uit in opdracht van en binnen de kaders (doel en middelen) die door u als klant (verwerkingsverantwoordelijke) zijn bepaald.



## 4.2 GRONDSLAG

Persoonsgegevens mogen alleen verwerkt worden als daar een reden voor is. De AVG geeft 6 grondslagen om persoonsgegevens te mogen verwerken, waarvan 'uitvoering van een overeenkomst' de grondslag is waarop Robidus haar verwerking baseert. Robidus verwerkt persoonsgegevens alleen daar waar zij noodzakelijk zijn voor de uitvoering van onze dienstverlening in het kader van de met u afgesloten overeenkomst.

## 4.3 DOELBINDING EN NOODZAKELIJKHEID

De verwerking van persoonsgegevens is alleen toegestaan voor zover dit noodzakelijk is voor het bereiken van een specifiek doel. Robidus verwerkt persoonsgegevens alleen voor de uitvoering van de dienstverlening die u als klant bij ons afneemt. De dienstverlening wordt nauwkeurig omschreven in de overeenkomst, zodat hieruit het verwerkingsdoel duidelijk blijkt. Afspraken over de verwerking van persoonsgegevens leggen we met u vast in een verwerkers-overeenkomst.



## 4.4 BEZWAARtermijnen

In de AVG wordt uitgegaan van twee rollen als het gaat om de verwerking van persoonsgegevens, namelijk de verwerkingsverantwoordelijke en de verwerker. Robidus is verwerker en voert haar dienstverlening uit in opdracht van en binnen de kaders (doel en middelen) die door u als klant (verwerkingsverantwoordelijke) zijn bepaald.

Categorie	Bezwaartermijn	Bron (indien beschikbaar)
Werkgeversdata	Maximaal totdat de dataset overschreven wordt als gevolg van beschikbaarstelling van de meest actuele dataset door werkgever	
Offertes	Maximaal 1 jaar na offerte-aanvraag	
Klantcontactgegevens	Maximaal 1 jaar na beëindiging klantrelatie of afwijzing van uitgebrachte offerte	
SV Subsidieregelingen	Maximaal 7 jaar na toepassing subsidie	Art. 52 lid 1 jo. art. 52 lid 4 AWR
Administratieve verzuim- en reïntegratiegegevens	Maximaal 2 jaar na beëindiging van de arbeidsrelatie	Beleidsregels van de Autoriteit Persoonsgegevens: 'De zieke werknemer'.
Administratieve ZW- en reïntegratiegegevens (ERD)	Maximaal 5 jaar na beëindiging van de arbeidsrelatie. Waarbij de termijn gaat lopen op 1 januari van het kalenderjaar volgend op het jaar waarin de arbeidsrelatie is beëindigd	Art. 3 lid 2 sub b Besluit werkzaamheden, administratieve voorschriften en kosten eigenrisico-dragen
Administratieve WGA- en reïntegratiegegevens (ERD)	Maximaal 10 jaar na ingangsdatum van de WIA-uitkering. Maximaal 5 jaar na WIA-beëindiging of afwijzing	Beleidsregels van de Autoriteit Persoonsgegevens: 'De zieke werknemer'
Specificaties UWV i.h.k.v. ERD WGA	Maximaal 7 jaar na beëindiging van activiteiten met betrekking tot claimafhandeling die voortvloeien uit verzekeringscontract betreffende ERD WGA	Art. 52 lid 1 jo. art. 52 lid 4 AWR
Gegevens bezwaar/ beroep/ aansprakelijkstelling	Fysieke dossiers maximaal 3 maanden na afloop van de juridische procedure* Digitale dossiers maximaal 5 jaar na afloop van de juridische procedure	Art. 7:412 BW
Back-ups servers	Minimaal 35 dagen na maken van de back-up	Contractuele afspraak met hostingpartij
Ongestructureerde data	7 jaar	

*\*De termijn van 3 maanden is een praktische richtlijn, vanwege de ruimte die fysieke dossiers innemen. Deze termijn wijkt om die reden af van de termijn van 5 jaar die gehanteerd wordt bij digitale dossiers.*

## 4.5 ISSUEMANAGEMENT

Bij de uitvoering van onze dienstverlening maken we gebruik van een aantal leveranciers die kwalificeren als subverwerker. Met al onze subverwerkers hebben wij een dienstverleningsovereenkomst, Service Level Agreement (SLA) en verwerkersovereenkomst afgesloten. Onze subverwerkers voldoen aan minimaal dezelfde informatiebeveiligings-eisen als Robidus. Onze subverwerkers staan uitgewerkt in de verwerkersovereenkomst die wij met onze klanten afsluiten. Indien Robidus voornemens is een nieuwe subverwerker in te zetten, dan informeren wij u over dit voornemen.

## 4.6 RECHTEN VAN BETROKKENEN

De AVG geeft betrokkenen, de personen van wie persoonsgegevens worden verwerkt, een aantal privacyrechten waarmee zij meer controle hebben over wat een organisatie van hen weet.

Als een betrokkene gebruik maakt van zijn privacyrechten en Robidus hiertoe een verzoek ontvangt, dan wordt deze in behandeling genomen. Voor de afhandeling van verzoeken van betrokkenen hanteert Robidus de volgende richtlijnen:

- Bij directe verzoeken aan Robidus vindt overleg plaats met u als klant, waarna u het verzoek ofwel zelf oppakt (eventueel met ondersteuning van Robidus), ofwel toestemming geeft aan Robidus om het verzoek af te handelen.
- Verzoeken van betrokkenen worden binnen één maand na ontvangst afgehandeld. Als afhandeling binnen 1 maand niet mogelijk is, wordt betrokkene op de hoogte gesteld van de aangepaste termijn van afhandeling, welke niet langer mag zijn dan drie maanden. Van de afhandeling ontvangt betrokkene een bevestiging.
- Er is een proces Verzoeken van betrokkenen ingericht voor de te volgen stappen.